

## CLAIMS

1. A safety judgment method for judging safety of an information processing apparatus among the information processing apparatus, a first authentication apparatus and a second authentication apparatus which are connected through a communication network, comprising the steps of:

receiving biological information by said information processing apparatus;

authenticating the biological information by judging whether the received biological information is proper or not by said information processing apparatus, said first authentication apparatus, or said second authentication apparatus;

collecting environment information including information about peripheral equipment connected to said information processing apparatus or about software installed in said information processing apparatus;

transmitting the collected environment information from said information processing apparatus to said first authentication apparatus;

transmitting an electronic certificate issued in advance by said second authentication apparatus and information encrypted with a secret key issued by said second authentication apparatus from said information processing apparatus to said first authentication apparatus;

authenticating the electronic certificate by said first authentication apparatus by decrypting the encrypted information with a public key acquired from the transmitted electronic certificate by using a public key acquired from said second authentication apparatus, and judging whether or not the decrypted information is proper;

authenticating the environment information by said first authentication apparatus by judging whether or not the transmitted environment information is proper with reference to an environment information database, which stores environment conditions classified according to information to be transmitted and received, and the transmitted information; and

judging said information processing apparatus to be safe by said first authentication apparatus when all the authentications performed in the step of authenticating the biological information, the step of authenticating the environment information, and the step of authenticating an electronic certificate are successful.

2. The safety judgment method as set forth in Claim 1, further comprising the sub-steps of:

receiving biological information by said first authentication apparatus;

authenticating the biological information by judging whether the received biological information is proper or not by said information processing apparatus, said first authentication

apparatus, or said second authentication apparatus;

collecting environment information including information about peripheral equipment connected to said first authentication apparatus or about software installed in said first authentication apparatus;

encrypting the environment information collected in the sub-step of collecting the environment information, with a secret key issued by said second authentication apparatus;

transmitting an electronic certificate issued by said second authentication apparatus and the encrypted environment information to said information processing apparatus;

authenticating the electronic certificate by said information processing apparatus by decrypting the encrypted environment information with a public key, which is acquired from the transmitted electronic certificate by using a public key acquired from said second authentication apparatus, and judging whether or not the decrypted environment information is proper;

authenticating the environment information by said information processing apparatus by judging whether or not the transmitted environment information is proper with reference to a sub-environment information database, which stores environment conditions classified according to information to be transmitted and received, and the decrypted environment information; and

judging said information processing apparatus and said first authentication apparatus to be safe when all the

authentications performed in the sub-step of authenticating the biological information, the sub-step of authenticating the environment information and the sub-step of authenticating the electronic certificate are successful and said information processing apparatus is judged safe in the step of judging said information processing apparatus to be safe.

3. A safety judgment method for judging safety of an information processing apparatus among the information processing apparatus, a first authentication apparatus and a second authentication apparatus which are connected through a communication network, comprising the steps of:

receiving biological information by said information processing apparatus;

authenticating the biological information by judging whether the received biological information is proper or not by said information processing apparatus, said first authentication apparatus, or said second authentication apparatus;

collecting environment information including information about peripheral equipment connected to said information processing apparatus or about software installed in said information processing apparatus;

encrypting the collected environment information with a secret key issued by said second authentication apparatus;

transmitting an electronic certificate issued in advance by

said second authentication apparatus and the environment information encrypted with the secret key from said information processing apparatus to said first authentication apparatus;

authenticating the electronic certificate by said first authentication apparatus by decrypting the encrypted environment information with a public key acquired from the transmitted electronic certificate by using a public key acquired from said second authentication apparatus, and judging whether or not the decrypted environment information is proper;

authenticating the environment information by said first authentication apparatus by judging whether or not the decrypted environment information is proper with reference to an environment information database, which stores environment conditions classified according to information to be transmitted and received, and the transmitted information; and

judging said information processing apparatus to be safe by said first authentication apparatus when all the authentications performed in the step of authenticating the biological information, the step of authenticating the environment information, and the step of authenticating an electronic certificate are successful.

4. The safety judgment method as set forth in Claim 3, further comprising the sub-steps of:

receiving biological information by said first authentication apparatus;

authenticating the biological information by judging whether the received biological information is proper or not by said information processing apparatus, said first authentication apparatus, or said second authentication apparatus;

collecting environment information including information about peripheral equipment connected to said first authentication apparatus or about software installed in said first authentication apparatus;

encrypting the environment information collected in the sub-step of collecting the environment information, with a secret key issued by said second authentication apparatus;

transmitting an electronic certificate issued by said second authentication apparatus and the encrypted environment information to said information processing apparatus;

authenticating the electronic certificate by said information processing apparatus by decrypting the encrypted environment information with a public key, which is acquired from the transmitted electronic certificate by using a public key acquired from said second authentication apparatus, and judging whether or not the decrypted environment information is proper;

authenticating the environment information by said information processing apparatus by judging whether or not the transmitted environment information is proper with reference to a sub-environment information database, which stores environment conditions classified according to information to be transmitted and

received, and the decrypted environment information; and  
judging said information processing apparatus and said first authentication apparatus to be safe when all the authentications performed in the sub-step of authenticating the biological information, the sub-step of authenticating the environment information and the sub-step of authenticating the electronic certificate are successful and said information processing apparatus is judged safe in the step of judging said information processing apparatus to be safe.

5. A safety judgment method for judging safety of an information processing apparatus among the information processing apparatus, a first authentication apparatus and a second authentication apparatus which are connected through a communication network, comprising the steps of:

receiving biological information by said information processing apparatus;

authenticating the biological information by judging whether the received biological information is proper or not by said information processing apparatus, said first authentication apparatus, or said second authentication apparatus;

collecting environment information including information about peripheral equipment connected to said information processing apparatus or about software installed in said information processing apparatus;

transmitting the collected environment information from said information processing apparatus to said first authentication apparatus;

transmitting an electronic certificate issued in advance by said second authentication apparatus and information encrypted with a secret key issued by said second authentication apparatus from said information processing apparatus to said first authentication apparatus;

authenticating the environment information by said first authentication apparatus by judging whether or not the transmitted environment information is proper with reference to an environment information database that stores environment conditions classified according to information to be transmitted and received; and

authenticating the electronic certificate by said information processing apparatus by decrypting the encrypted software with a public key, which is acquired from the transmitted electronic certificate by using a public key acquired from said second authentication apparatus, and judging whether or not the decrypted software is proper; and

installing the decrypted software in said information processing apparatus when all the authentications performed in the step of authenticating the biological information, the step of authenticating the environment information and the step of authenticating the electronic certificate are successful.



6. A safety judgment system for judging safety of an information processing apparatus among the information processing apparatus, a first authentication apparatus and a second authentication apparatus which are connected through a communication network, wherein

said information processing apparatus comprises: biological information receiving means for receiving biological information; biological information authenticating means for judging whether or not the received biological information is proper; environment information collecting means for collecting environment information including information about peripheral equipment connected thereto or about software installed therein; environment information transmitting means for transmitting the environment information collected by said environment information collecting means to said first authentication apparatus; and encrypted information transmitting means for transmitting an electronic certificate issued by said second authentication apparatus and information encrypted with a secret key issued by said second authentication apparatus to said first authentication apparatus, and

said first authentication apparatus comprises: electronic certificate authenticating means for decrypting the encrypted information with a public key, which is acquired from the transmitted electronic certificate by using a public key acquired

from said second authentication apparatus, and judging whether or not the decrypted information is proper; environment information authenticating means for judging whether or not the transmitted environment information is proper with reference to an environment information database, which stores environment conditions classified according to information to be transmitted and received, and the transmitted information; and safety judging means for judging said information processing apparatus to be safe when all the authentications performed by said biological information authenticating means, said environment information authenticating means and said electronic certificate authenticating means are successful.

7. The safety judgment system as set forth in Claim 6, wherein said environment information transmitting means and said encrypted information transmitting means are constructed to encrypt the collected environment information with said secret key and transmit the encrypted environment information together with said electronic certificate to said first authentication apparatus.

8. The safety judgment system as set forth in Claim 6, further comprising a shop computer for transmitting and receiving information relating to transactions to/from said information processing apparatus, wherein

said information processing apparatus further comprises

means for receiving information relating to transactions, including product information or price information,

said encrypted information transmitting means is constructed to transmit an electronic certificate issued by said second authentication apparatus and the information relating to transactions encrypted with said secret key issued by said second authentication apparatus to said first authentication apparatus,

said environment information authenticating means is constructed to read an environment condition related to a class corresponding to the transmitted product information or price information from said environment information database and judge whether or not the environment condition is proper, based on whether or not the transmitted environment information matches the read environment condition, and

said first authentication apparatus further comprises means for transmitting information indicating that said information processing apparatus is safe to said shop computer, when said safety judging means judges that said information processing apparatus is safe.

9. The safety judgment system as set forth in Claim 6, wherein

said first authentication apparatus comprises:  
sub-biological information receiving means for receiving biological information; sub-biological information authenticating means for

judging whether or not the biological information received by said sub-biological information receiving means is proper;  
sub-environment information collecting means for collecting environment information including information about peripheral equipment connected thereto or about software installed therein;  
sub-encrypting means for encrypting the environment information collected by said sub-environment information collecting means, with a secret key issued by said second authentication apparatus;  
and sub-encrypted information transmitting means for transmitting an electronic certificate issued by said second authentication apparatus and the encrypted environment information to said information processing apparatus, and

said information processing apparatus comprises:  
sub-electronic certificate authenticating means for decrypting the encrypted environment information with a public key, which is acquired from the transmitted electronic certificate by using a public key acquired from said second authentication apparatus, and  
judging whether or not the decrypted environment information is proper; sub-environment information authenticating means for judging whether or not the transmitted environment information is proper with reference to a sub-environment information database, which stores environment conditions classified according to information to be transmitted and received, and the decrypted environment information; and sub-safety judging means for judging said information processing apparatus and said first authentication

apparatus to be safe when all the authentications performed by said sub-biological information authenticating means, said sub-environment information authenticating means and said sub-electronic certificate authenticating means are successful and said safety judging means judges that said information processing apparatus are safe.

10. The safety judgment system as set forth in Claim 9, wherein the environment information includes information about name or version of installed software, equipment name or version of connected peripheral equipment, or device name or version of said information processing apparatus.

11. The safety judgment system as set forth in Claim 10, wherein the biological information is information about voice, fingerprint, retina, or iris.

12. A safety judgment system for judging safety of an information processing apparatus among the information processing apparatus, a first authentication apparatus and a second authentication apparatus which are connected through a communication network, wherein

said information processing apparatus comprises a processor capable of performing the operations of:

receiving biological information;

authenticating the biological information by judging whether or not the received biological information is proper;

collecting environment information including information about peripheral equipment connected to said information processing apparatus or about software installed in said information processing apparatus;

transmitting the collected environment information to said first authentication apparatus; and

transmitting an electronic certificate issued by said second authentication apparatus and information encrypted with a secret key issued by said second authentication apparatus to said first authentication apparatus, and

said first authentication apparatus comprises a processor capable of performing the operations of:

authenticating the electronic certificate by decrypting the encrypted information with a public key, which is acquired from the transmitted electronic certificate by using a public key acquired from said second authentication apparatus, and judging whether or not the decrypted information is proper;

authenticating the environment information by judging whether or not the transmitted environment information is proper with reference to an environment information database, which stores environment conditions classified according to information to be transmitted and received, and the transmitted information; and

judging said information processing apparatus to be safe

when all the authentications by the operation of authenticating the biological information, the operation of authenticating the environment information and the operation of authenticating the electronic certificate are successful.

13. The safety judgment system as set forth in Claim 12, wherein the processor of said information processing apparatus is further capable of performing the operation of encrypting the collected environment information with the secret key and transmitting the encrypted environment information together with the electronic certificate to said first authentication apparatus.

14. The safety judgment system as set forth in Claim 12, further comprising a shop computer for transmitting and receiving information relating to transactions to/from said information processing apparatus, wherein

the processor of said information processing apparatus is further capable of performing the operations of:

receiving information relating to transactions, including product information or price information;

transmitting an electronic certificate issued by said second authentication apparatus, and the information relating to transactions encrypted with a secret key issued by said second authentication apparatus to said first authentication apparatus; and

reading an environment condition related to a class corresponding to the transmitted product information or price information from the environment information database and judging whether or not the environment condition is proper, based on whether or not the transmitted environment information matches the read environment condition, and

the processor of said first authentication apparatus is further capable of performing the operation of transmitting information indicating that said information processing apparatus is safe to said shop computer, when the information processing apparatus is judged safe in the operation of judging said information processing apparatus to be safe.

15. The safety judgment system as set forth in Claim 12, wherein

the processor of said first authentication apparatus is further capable of performing the sub-operations of:

receiving biological information;

authenticating the biological information by judging whether or not the received biological information is proper;

collecting environment information including information about peripheral equipment connected to said first authentication apparatus or about software installed in said first authentication apparatus;

encrypting the collected environment information with a



secret key issued by said second authentication apparatus; and

transmitting an electronic certificate issued by said second authentication apparatus and the encrypted environment information to said information processing apparatus, and

the processor of said information processing apparatus is further capable of performing the sub-operations of:

authenticating the electronic certificate by decrypting the encrypted environment information with a public key, which is acquired from the transmitted electronic certificate by using a public key acquired from said second authentication apparatus, and judging whether or not the decrypted environment information is proper;

authenticating the environment information by judging whether or not the transmitted environment information is proper with reference to a sub-environment information database, which stores environment conditions classified according to information to be transmitted and received, and the decrypted environment information; and

judging said information processing apparatus and said first authentication apparatus to be safe when all the authentications by the sub-operation of authenticating the biological information, the sub-operation of authenticating the environment information and the sub-operation of authenticating the electronic certificate are successful and said information processing apparatus is judged safe in the operation of judging said

information processing apparatus to be safe.

16. The safety judgment system as set forth in Claim 15, wherein the environment information includes information about name or version of installed software, equipment name or version of connected peripheral equipment, or device name or version of said information processing apparatus.

17. The safety judgment system as set forth in Claim 16, wherein the biological information is information about voice, fingerprint, retina, or iris.

18. A safety judgment system for judging safety of an information processing apparatus among the information processing apparatus, a first authentication apparatus and a second authentication apparatus which are connected through a communication network, wherein

said information processing apparatus comprises: biological information receiving means for receiving biological information; biological information authenticating means for judging whether or not the biological information received by said biological information receiving means is proper; environment information collecting means for collecting environment information including information about peripheral equipment connected thereto or about software installed therein; and environment information

transmitting means for transmitting the environment information collected by said environment information collecting means to said first authentication apparatus,

said first authentication apparatus comprises: encrypted information transmitting means for transmitting an electronic certificate issued by said second authentication apparatus and software encrypted with a secret key issued by said second authentication apparatus to said information processing apparatus; and environment information authenticating means for judging whether or not the transmitted environment information is proper with reference to an environment information database that stores environment conditions classified according to information to be transmitted and received, and

said information processing apparatus further comprises: electronic certificate authenticating means for decrypting the encrypted software with a public key, which is acquired from the transmitted electronic certificate by using a public key acquired from said second authentication apparatus, and judging whether or not the decrypted software is proper; and installing means for installing the decrypted software when all the authentications performed by said biological information authenticating means, said environment information authenticating means and said electronic certificate authenticating means are successful.

19. The safety judgment system as set forth in Claim 18,

wherein said information processing apparatus further comprises:

main power supplying means;

sub-power supplying means;

communicating means for reception for receiving supply of power from said sub-power supplying means; and

storing means for storing the electronic certificate and software encrypted with the secret key which were transmitted by said encrypted information transmitting means and received by said communicating means for reception, when power is not supplied by said main power supplying means.

20. The safety judgment system as set forth in Claim 19, wherein said electronic certificate authenticating means is constructed to read the electronic certificate and software stored in said storing means when power is supplied by said main power supplying means, decrypt the encrypted software with a public key which is acquired from the electronic certificate by using a public key acquired from said second authentication apparatus, and judge whether or not the decrypted software is proper.

21. The safety judgment system as set forth in Claim 20, wherein said software is patch software for software pre-installed in said information processing apparatus.

22. The safety judgment system as set forth in Claim 20,

wherein said information processing apparatus further comprises deleting means for deleting data stored in a storage unit on and after a predetermined time, when the software installed by said installing means is executed.

23. The safety judgment system as set forth in Claim 22, wherein the environment information includes information about name or version of installed software, equipment name or version of connected peripheral equipment, or device name or version of said information processing apparatus.

24. The safety judgment system as set forth in Claims 23, wherein the biological information is information about voice, fingerprint, retina, or iris.

25. A safety judgment system for judging safety of an information processing apparatus among the information processing apparatus, a first authentication apparatus and a second authentication apparatus which are connected through a communication network, wherein

said information processing apparatus comprises a processor capable of performing the operations of:

receiving biological information;

authenticating the biological information by judging whether or not the received biological information is proper;

collecting environment information including information about peripheral equipment connected to said information processing apparatus or about software installed in said information processing apparatus; and

transmitting the collected environment information to said first authentication apparatus, and

said first authentication apparatus comprises a processor capable of performing the operations of:

transmitting an electronic certificate issued by said second authentication apparatus and software encrypted with a secret key issued by said second authentication apparatus to said information processing apparatus; and

authenticating the environment information by judging whether or not the transmitted environment information is proper with reference to an environment information database that stores environment conditions classified according to information to be transmitted and received, and

said processor of said information processing apparatus is further capable of performing the operations of:

authenticating the electronic certificate by decrypting the encrypted software with a public key, which is acquired from the transmitted electronic certificate by using a public key acquired from said second authentication apparatus, and judging whether or not the decrypted software is proper; and

installing the decrypted software when all the

authentications by the operation of authenticating the biological information, the operation of authenticating the environment information and the operation of authenticating the electronic certificate are successful.

26. The safety judgment system as set forth in Claim 25, wherein the processor of said information processing apparatus is further capable of performing the operations of:

causing main power supplying means to supply main power;

causing sub-power supplying means to supply sub power;

supplying power from said sub-power supplying means to communicating means for reception; and

causing said communicating means for reception to receive the transmitted electronic certificate and software encrypted with the secret key, and store the electronic certificate and software in storing means, when power is not supplied by said main power supplying means.

27. The safety judgment system as set forth in Claim 26, wherein the processor of said information processing apparatus is further capable of performing the operation of reading the electronic certificate and software stored in said storing means when power is supplied by said main power supplying means, decrypting the encrypted software with a public key, which is acquired from the

electronic certificate by using a public key acquired from said second authentication apparatus, and judging whether or not the decrypted software is proper.

28. The safety judgment system as set forth in Claim 27, wherein the software is patch software for software pre-installed in said information processing apparatus.

29. The safety judgment system as set forth in Claim 27, wherein the processor of said information processing apparatus is further capable of performing the operation of deleting data stored in a storage unit on and after a predetermined time from said storage unit when the installed software is executed.

30. The safety judgment system as set forth in Claim 29, wherein the environment information includes information about name or version of installed software, equipment name or version of connected peripheral equipment, or device name or version of said information processing apparatus.

31. The safety judgment system as set forth in Claim 30, wherein the biological information is information about voice, fingerprint, retina, or iris.

32. A safety judgment system for judging safety of an



information processing apparatus among the information processing apparatus, a first authentication apparatus and a second authentication apparatus which are connected through a communication network, wherein

said information processing apparatus comprises: biological information receiving means for receiving biological information; environment information collecting means for collecting environment information including information about peripheral equipment connected thereto or about software installed therein; encrypting means for encrypting the biological information received by said biological information receiving means and the environment information collected by said environment information collecting means, with a secret key issued by said second authentication apparatus; and encrypted information transmitting means for transmitting an electronic certificate issued by said second authentication apparatus and the encrypted biological information and environment information to said first authentication apparatus, and

said first authentication apparatus comprises: electronic certificate authenticating means for decrypting the encrypted biological information and environment information with a public key, which is acquired from the transmitted electronic certificate by using a public key acquired from said second authentication apparatus, and judging whether or not the decrypted biological information and environment information are proper; environment

information authenticating means for judging whether or not the transmitted environment information is proper with reference to an environment information database, which stores environment conditions classified according to information to be transmitted and received, and the decrypted environment information; biological information authenticating means for judging whether or not the biological information is proper by comparing the decrypted biological information with pre-stored biological information; and safety judging means for judging said information processing apparatus to be safe when all the authentications performed by said biological information authenticating means, said environment information authenticating means and said electronic certificate authenticating means are successful.

33. The safety judgment system as set forth in Claim 32, wherein

said first authentication apparatus comprises:

sub-biological information receiving means for receiving biological information; sub-biological information authenticating means for judging whether or not the biological information received by said sub-biological information receiving means is proper;

sub-environment information collecting means for collecting environment information including information about peripheral equipment connected thereto or about software installed therein; sub-encrypting means for encrypting the environment information

collected by said sub-environment information collecting means, with a secret key issued by said second authentication apparatus; and sub-encrypted information transmitting means for transmitting an electronic certificate issued by said second authentication apparatus and the encrypted environment information to said information processing apparatus, and

said information processing apparatus comprises:

sub-electronic certificate authenticating means for decrypting the encrypted environment information with a public key, which is acquired from the transmitted electronic certificate by using a public key acquired from said second authentication apparatus, and judging whether or not the decrypted environment information is proper; sub-environment information authenticating means for judging whether or not the transmitted environment information is proper with reference to a sub-environment information database, which stores environment conditions classified according to information to be transmitted and received, and the decrypted environment information; and sub-safety judging means for judging said information processing apparatus and said first authentication apparatus to be safe when all the authentications performed by said sub-biological information authenticating means, said sub-environment information authenticating means and said sub-electronic certificate authenticating means are successful and said safety judging means judges that said information processing apparatus is safe.

34. The safety judgment system as set forth in Claim 33, wherein the environment information includes information about name or version of installed software, equipment name or version of connected peripheral equipment, or device name or version of said information processing apparatus.

35. The safety judgment system as set forth in Claim 34, wherein the biological information is information about voice, fingerprint, retina, or iris.

36. A safety judgment system for judging safety of an information processing apparatus among the information processing apparatus, a first authentication apparatus and a second authentication apparatus which are connected through a communication network, wherein

said information processing apparatus comprises a processor capable of performing the operations of:

receiving biological information;

collecting environment information including information about peripheral equipment connected to said information processing apparatus or about software installed in said information processing apparatus;

encrypting the received biological information and the collected environment information with a secret key issued by said

second authentication apparatus; and

transmitting an electronic certificate issued by said second authentication apparatus and the encrypted biological information and environment information to said first authentication apparatus, and

said first authentication apparatus comprises a processor capable of performing the operations of:

authenticating the electronic certificate by decrypting the encrypted biological information and environment information with a public key, which is acquired from the transmitted electronic certificate by using a public key acquired from said second authentication apparatus, and judging whether or not the decrypted biological information and environment information are proper;

authenticating the environment information by judging whether or not the transmitted environment information is proper with reference to an environment information database, which stores environment conditions classified according to information to be transmitted and received, and the decrypted environment information;

authenticating the biological information by judging whether or not the decrypted biological information is proper by comparing the decrypted biological information with pre-stored biological information; and

judging said information processing apparatus to be safe when all the authentications by the operation of authenticating the

biological information, the operation of authenticating the environment information and the operation of authenticating the electronic certificate are successful.

37. The safety judgment system as set forth in Claim 36, wherein

the processor of said first authentication apparatus is capable of performing the sub-operations of:

receiving biological information;

judging whether or not the received biological information is proper;

collecting environment information including information about peripheral equipment connected to said first authentication apparatus or about software installed in said first authentication apparatus;

encrypting the collected environment information with a secret key issued by said second authentication apparatus; and

transmitting an electronic certificate issued by said second authentication apparatus and the encrypted environment information to said information processing apparatus, and

the processor of said information processing apparatus is capable of performing the sub-operations of:

decrypting the encrypted environment information with a public key, which is acquired from the transmitted electronic certificate by using a public key acquired from said second

authentication apparatus, and judging whether or not the decrypted environment information is proper;

judging whether or not the transmitted environment information is proper with reference to a sub-environment information database, which stores environment conditions classified according to information to be transmitted and received, and the decrypted environment information; and

judging said information processing apparatus and said first authentication apparatus to be safe when all the authentications by the sub-operation of authenticating the biological information, the sub-operation of authenticating the environment information, and the sub-operation of authenticating the electronic certificate are judged successful, and said information processing apparatus is judged safe in the operation of judging safety.

38. The safety judgment system as set forth in Claim 37, wherein the environment information includes information about name or version of installed software, equipment name or version of connected peripheral equipment, or device name or version of said information processing apparatus.

39. The safety judgment system as set forth in Claim 38, wherein the biological information is information about voice, fingerprint, retina, or iris.

40. A safety judgment apparatus for judging safety of an information processing apparatus connected to a first authentication apparatus and a second authentication apparatus through a communication network, comprising:

biological information authenticating means for judging whether or not received biological information is proper;

environment information collecting means for collecting environment information including information about peripheral equipment connected to said information processing apparatus or about software installed in said information processing apparatus;

environment information transmitting means for transmitting the environment information collected by said environment information collecting means to said first authentication apparatus;

encrypted information transmitting means for transmitting an electronic certificate issued by said second authentication apparatus and information encrypted with a secret key issued by said second authentication apparatus to said first authentication apparatus; and

safety judging means for judging said information processing apparatus to be safe when said biological information authenticating means judges proper, said first authentication apparatus judges that the environment information transmitted by said environment information transmitting means is proper, said



first authentication apparatus judges that the electronic certificate and encrypted information transmitted by said encrypted information transmitting means are proper, and said safety judging means receives information indicating that the information is proper.

41. A safety judgment apparatus for judging safety of an information processing apparatus connected to a first authentication apparatus and a second authentication apparatus through a communication network, comprising:

biological information authenticating means for judging whether or not received biological information is proper;

environment information collecting means for collecting environment information including information about peripheral equipment connected to said information processing apparatus or about software installed in said information processing apparatus;

environment information transmitting means for transmitting the environment information collected by said environment information collecting means to said first authentication apparatus;

electronic certificate authenticating means for, when an electronic certificate and encrypted software are received from said first authentication apparatus, decrypting the encrypted software with a public key, which is acquired from the electronic certificate by using a public key acquired from said second authentication

apparatus, and judging whether or not the decrypted software is proper; and

installing means for installing the decrypted software in said information processing apparatus when the authentications performed by said biological information authenticating means and said electronic certificate authenticating means are judged successful, said first authentication apparatus judges that the environment information transmitted by said environment information transmitting means is proper, and said installing means receives information indicating that the information is proper.

42. A safety judgment apparatus for judging safety of an information processing apparatus connected to a first authentication apparatus and a second authentication apparatus through a communication network, comprising a processor capable of performing the operations of:

authenticating biological information by judging whether or not received biological information is proper;

collecting environment information including information about peripheral equipment connected to said information processing apparatus or about software installed in said information processing apparatus;

transmitting the collected environment information to said first authentication apparatus;

transmitting an electronic certificate issued by said second authentication apparatus and information encrypted with a secret key issued by said second authentication apparatus to said first authentication apparatus; and

judging said information processing apparatus to be safe when the biological information is judged proper in the operation of authenticating the biological information, said first authentication apparatus judges that the transmitted environment information is proper, the first authentication apparatus judges that the transmitted electronic certificate and encrypted information are proper, and information indicating that the information is proper is received.

43. A safety judgment apparatus for judging safety of an information processing apparatus connected to a first authentication apparatus and a second authentication apparatus through a communication network, comprising a processor capable of performing the operations of:

authenticating biological information by judging whether or not received biological information is proper;

collecting environment information including information about peripheral equipment connected to said information processing apparatus or about software installed in said information processing apparatus;

transmitting the collected environment information to said

first authentication apparatus;

when an electronic certificate and encrypted software are received from said first authentication apparatus, authenticating the electronic certificate by decrypting the encrypted software with a public key, which is acquired from the electronic certificate by using a public key acquired from said second authentication apparatus, and judging whether or not the decrypted software is proper; and

installing the decrypted software in said information processing apparatus when authentications are judged successful in the operation of authenticating the biological information and the operation of authenticating the electronic certificate, said first authentication apparatus judges that transmitted environment information is proper, and information indicating that the information is proper is received.

44. A first authentication apparatus for judging safety of an information processing apparatus connected through a communication network, comprising:

authentication information receiving means for receiving authentication information indicating whether or not biological information received by said information processing apparatus is proper;

electronic certificate authenticating means for, when an electronic certificate issued by a second authentication apparatus

connected through the communication network and information encrypted with a secret key issued by said second authentication apparatus are transmitted from said information processing apparatus, decrypting the encrypted information with a public key, which is acquired from the transmitted electronic certificate by using a public key acquired from said second authentication apparatus, and judging whether or not the decrypted information is proper;

environment information authenticating means for, when environment information including information about peripheral equipment connected to said information processing apparatus or about software installed in said information processing apparatus is received from said information processing apparatus, judging whether or not the received environment information is proper with reference to an environment information database, which stores environment conditions classified according to information to be transmitted and received, and the transmitted information; and

safety judging means for judging said information processing apparatus to be safe when said authentication information receiving means receives authentication information indicating that the biological information is proper, and authentications performed by said environment information authenticating means and said electronic certificate authenticating means are judged successful.

45. A first authentication apparatus for judging safety of an information processing apparatus connected through a communication network, comprising a processor capable of performing the operations of:

receiving authentication information indicating whether or not biological information received by said information processing apparatus is proper;

when an electronic certificate issued by a second authentication apparatus connected through the communication network and information encrypted with a secret key issued by said second authentication apparatus are transmitted from said information processing apparatus, authenticating the electronic certificate by decrypting the encrypted information with a public key, which is acquired from the transmitted electronic certificate by using a public key acquired from said second authentication apparatus, and judging whether or not the decrypted information is proper;

when environment information including information about peripheral equipment connected to said information processing apparatus or about software installed in said information processing apparatus is received from said information processing apparatus, authenticating the environment information by judging whether or not the received environment information is proper with reference to an environment information database, which stores environment conditions classified according to

information to be transmitted and received, and the transmitted information; and

judging said information processing apparatus to be safe when authentication information indicating that the biological information is proper is received, and the authentications by the operation of authenticating the environment information and the operation of authenticating the electronic certificate are judged successful.

46. A computer program product, within a computer readable medium, for judging safety of a computer connected to a first authentication apparatus and a second authentication apparatus through a communication network, comprising the steps of:

causing the computer to authenticate biological information by authenticating whether or not received biological information is proper;

causing the computer to collect environment information including information about connected peripheral equipment or about installed software;

causing the computer to transmit environment information by transmitting the collected environment information to said first authentication apparatus;

causing the computer to transmit encrypted information by transmitting an electronic certificate issued by said second

authentication apparatus and information encrypted with a secret key issued by said second authentication apparatus to said first authentication apparatus; and

causing the computer to judge the computer to be safe when the biological information is judged proper in the step of authenticating the biological information, the first authentication apparatus judges that environment information transmitted in the step of transmitting environment information is proper, the first authentication apparatus judges that the electronic certificate and encrypted information transmitted in the step of transmitting the encrypted information are proper, and information indicating that the information is proper is received from said first authentication apparatus.

47. A computer program product, within a computer readable medium, for judging safety of a computer connected to a first authentication apparatus and a second authentication apparatus through a communication network, comprising the steps of:

causing the computer to authenticate biological information by authenticating whether or not received biological information is proper;

causing the computer to collect environment information including information about connected peripheral equipment or about installed software;



causing the computer to transmit environment information by transmitting the collected environment information to said first authentication apparatus;

when an electronic certificate and encrypted software are received from said first authentication apparatus, causing the computer to authenticate the electronic certificate by decrypting the encrypted software with a public key, which is acquired from the electronic certificate by using a public key acquired from the second authentication apparatus, and judging whether or not the decrypted software is proper; and

causing the computer to install the decrypted software when authentications performed in the step of authenticating the biological information and the step of authenticating the electronic certificate are judged successful, the first authentication apparatus judges that the environment information transmitted in the step of transmitting environment information is proper, and information indicating that the information is proper is received.